SAND No. 2002-1068P

U.S. Laboratory Biosecurity Policy Paper

Prepared for:

Office of Homeland Security
Prevention and Preparedness Directorate
Medical and Public Health Preparedness PCC
National Bioterrorism Laboratory Working Group
Laboratory Biosecurity Subgroup

Prepared by:

Reynolds M. Salerno
Sandia National Laboratories
Albuquerque, New Mexico

February 2002

Issue

The possibility that the recent bioterrorism attacks in the U.S. were perpetrated by someone with access to a biological research laboratory has stimulated many efforts to tighten security at U.S. federal laboratories. In particular, the Kennedy-Frist Bioterrorism Preparedness Act of December 2001 (S. 1765) and the U.S. Appropriations Bill of September 2001 (H.R. 2500) require enhanced physical protection and security of biological pathogens at research laboratories in the U.S.

Unfortunately, no recommendations or standards exist domestically or internationally to guide those with responsibility for protecting high-consequence microbial agents and toxins. Laboratory directors have no guidelines against which to measure the effectiveness of their own security systems. As a result, heavy investments are now being made in traditional concepts of facility security that generally rely on perimeter fences and armed personnel – often described as "guns, gates, and guards." Currently, there is no uniformity to the security upgrades under consideration and implementation, and there is concern that many of these upgrades may not be mitigating vulnerabilities.

Unique Problem Deserves Unique Solution

There are several fundamental aspects of high-containment biological research that demonstrate why biosecurity should be differentiated from traditional concepts of high security. First, high-consequence pathogens (with the exception of smallpox) are not unique to any one facility or one country. Many of these organisms are ubiquitous in nature and exist in various quantities in laboratories around the world. This reasoning suggests that a terrorist organization would not likely target any one particular facility – unless it was judged to have especially inadequate security or a particularly virulent or fast growing strain of a pathogen that was not readily available somewhere else.

Second, at an active biomedical research facility, infectious material may be found at any time in a wide variety of places, such as storage freezers, laboratory incubators, living animals, animal excrement, or animal carcasses. Therefore, the absolute amount of any given organism in active biomedical research facilities cannot be reliably quantified from day to day.

Third, any quantity of a high-consequence pathogen is strategically significant. One viable microorganism can be cultured and weaponized with common, commercially available equipment. This circumstance, combined with the fact that pathogens emit no energy and thus cannot be detected at a distance with currently available technology, reveals how easy it would be for an individual with authorized access to a facility to remove a small amount of pathogenic material without raising suspicion of others. This person could then sell the dangerous pathogens to a would-be bioterrorist or become one himself. In other words, the effectiveness of a security system at a high-containment biological research laboratory will depend – first and foremost – on the integrity of the individuals who have access to the high-consequence pathogens.

Because of the unique nature of biomedical and microbiological research, extensive perimeter and inventory control systems may jeopardize critical research and will not provide adequate protection. High-consequence pathogens in the U.S. will remain at risk of theft or diversion. Precious resources of the U.S. Government will be wasted unless security guidelines are established that specifically address the unique targets, threats, and risks associated with biomedical research, and recognize the legitimate variation in operating procedures of sites that work with high-consequence microbial agents and toxins. Such an analysis will reveal that biomedical research requires a unique security methodology that does not currently exist.

A Multi-Agency Homeland Security Initiative

Another critical and unique element of biomedical research in the U.S. is that no one U.S. Government agency can claim a monopoly over it. In fact, the nature of biomedical research demands that various U.S. agencies – Health and Human Services, Defense, Agriculture, and Energy, among others – constantly cooperate, collaborate, and communicate with each other. All of these agencies, as well as many private companies and universities, store, use, and transport high-consequence pathogens. High-consequence pathogens are frequently shipped between laboratories of various agencies. Some laboratories even are physically co-located, and share research missions, with laboratories of other agencies. As a result, the security guidelines of one department will be meaningless unless they are supported and followed by all of the stakeholder agencies.

For this reason, as well as the increasing bioterrorism threat, an ad-hoc Interagency Working Group on Biosecurity (IWGB) was convened in January 2001 – well before the anthrax attacks in the U.S. – and has continued to meet regularly over the last 13 months. The IWGB's chartered mission is to improve biosecurity for high-consequence microbial agents and toxins. The IWGB's membership includes representatives from the U.S. Departments of Agriculture, Defense, Energy, Health and Human Services, Justice, and Transportation.

The IWGB believes that existing security standards must be tailored to adequately protect high-consequence microbial agents and toxins. In addition, the IWGB recognizes that developing effective and broadly applicable biosecurity guidelines will require contributions and commitments from U.S. Government experts in biomedical research, physical protection, law enforcement, transportation, and policy. The Office of Homeland Security is ideally positioned to oversee this multi-agency effort that would directly strengthen the U.S.'s defenses against bioterrorism. The Office of Homeland Security should officially charter the IWGB and adopt its mission.

Biosafety and Biosecurity

An important precedent for such an endeavor is the creation of biosafety standards. Throughout the U.S. biological research community, there is a strong culture and a well-established program of biosafety. With assistance from many biomedical scientists from a variety of agencies, the Centers for Disease Control and Prevention and the National

Institutes of Health published an extensive manual, *Biosafety in Microbiological and Biomedical Laboratories* (BMBL), on proper biosafety procedures and standards. Now in its fourth edition, the BMBL and its recommended guidelines are accepted as the international "gold standard" for safely conducting microbiological research. Since the BMBL's publication, there has been a significant reduction in the number of reported biosafety incidents in the U.S.

No manual for biosecurity analogous to the BMBL exists. However, many of the same biomedical scientists responsible for creating the BMBL are actively engaged in the IWGB initiative. The opportunity exists to build on the BMBL process and document a methodology that would provide effective security for high-consequence microbial agents and toxins.

The IWGB appreciates that the objectives and strategies of biosafety and biosecurity are different and should not be confused. *Biosafety* aims to reduce or eliminate exposure of laboratory workers or other persons and the outside environment to potentially hazardous agents involved in microbiological or biomedical facility research. Biosafety is achieved by implementing various degrees of laboratory "containment," or safe methods of managing infectious materials in a laboratory setting. There are three types of barriers that work together to establish containment: laboratory practice and technique, safety equipment (primary barriers), and facility design and construction (secondary barriers). Biosafety procedures and equipment do not protect against theft or diversion of high-consequence pathogens.

By contrast, the objective of *biosecurity* is to protect high-consequence microbial agents and toxins, or critical related information, against theft or diversion by those who intend to pursue bioterrorism or biological weapons proliferation. Biosecurity should be based on substantive assessments of biological targets, threats, risks and vulnerabilities, and should be achieved through the integration of specifically designed technologies, procedures, and protocols. A comprehensive biosecurity system would include many of the following elements:

- Physical protection
- Personnel reliability
- Adequate scientific program oversight
- Pathogen accountability
- Transportation security
- Information security

The IWGB formulated these elements of a biosecurity system, but it cannot yet make informed policy recommendations for implementing biosecurity. Such recommendations would evolve out of a concerted multi-agency effort to develop a biosecurity methodology and document biosecurity standards.

International Implications

Despite the absence of U.S. biosecurity guidelines, the U.S. Government's Concept Paper on "New Ways to Strengthen the International Regime Against Biological Weapons" recommends that internationally recognized and nationally implemented "security standards for pathogenic microorganisms" be considered as a one of many potential alternatives to the rejected verification protocol for the Biological Weapons Convention (BWC). Since international biosecurity standards do not exist, a U.S. biosecurity standard would likely be adopted by the international community and thus could serve as a significant component of international controls on biological weapons proliferation.